EL CONTROL DE ACCESOS TECNOLÓGICOS, UNA SOLUCIÓN PARA MINIMIZAR RIESGOS DE INTRUSIÓN EN LOS CONJUNTOS RESIDENCIALES

Javier Vargas Zarate

Universidad Militar Nueva Granada

Facultad De Relaciones Internacionales Estrategia y Seguridad

Especialización Administración y de la Seguridad

Bogotá, Colombia

2015

TALA DE CONTENIDO

TABLA DE GRÁFICOS

GLOSARIO

BIOMETRÍA: es una tecnología de seguridad basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas.

CONTROL DE ACCESO: es el conjunto de medios, normas y Acciones que tienen como finalidad, restringir o permitir el ingreso o salida de personas, animales o cosas.

CONTROL DE VISITANTES: es un sistema de control de acceso donde el visitante puede acceder a las áreas autorizadas mediante la huella o una tarjeta de proximidad dependiendo de las necesidades de seguridad de la empresa y la configuración del sistema de control de acceso.

CONTROL DE RESIDENTES: es un sistema que controla a los residentes de manera eficiente y rápida, estableciendo la diferencia.

CONTROL VEHICULAR: Se encarga de verificar que los vehículos que ingresen al conjunto.

CARNETIZACIÓN: actividad mediante la cual se elaboran y generan carnés

ELECTROIMÁN: es un tipo de imán en el que el campo magnético se produce mediante el flujo

INTRUSIÓN: acción de introducirse una persona o cosa en algo de forma indebida.

LECTORA: es el proceso de significación y comprensión de algún tipo de información y/o ideas almacenadas en un soporte y transmitidas mediante algún tipo de código

LECTORA DE PROXIMIDAD: son sensores de proximidad que detectan cuán cerca de superficies vecinas.

LOS SISTEMAS BIOMÉTRICOS DE HUELLAS DACTILARES: se utilizan las características únicas y los patrones de huellas digitales para una amplia variedad de usos. Estos sistemas escanean dichas huellas y las comparan con bases de datos conocidas en el sistema.

PLANTILLA: Es una forma compacta de representar un conjunto de muestras de una sola característica biométrica.

RIESGO: es una medida de la magnitud de los daños frente a una situación peligrosa

de una corriente eléctrica.

TARJETAS DE PROXIMIDAD: es el nombre genérico dado a la tarjeta inteligente "sin contacto" que se utiliza para el acceso seguro o como un sistema de pago.

TARJETAS DE BANDA MAGNÉTICA: son unas tarjetas que tienen una banda magnética con un código para identificarlas rápidamente

RESUMEN

Hoy en día el control de acceso más utilizado al personal que ingresa a los conjuntos residenciales, se realiza manualmente, donde el vigilante hace una llamada al apartamento hacia el cual se dirige, con el fin que autorice su ingreso, y si es autorizado lo registran en una bitácora, de la misma forma la información de los vehículos.

Actualmente se cuenta con diferentes sistemas para el acceso a conjuntos residenciales como: tarjetas magnéticas, sistemas biométricos (escaneo de huella digital, escaneo del iris, reconocimiento de voz, cara, oreja), algunos más costosos que otros.

Por lo anterior en este trabajo se describirán algunas herramientas utilizadas para el control de acceso que permiten controlar el nivel de seguridad en los conjuntos residenciales, de igual manera estos sistemas mantienen actualizada la base de datos del personal que ingresa.

Palabras claves: control de acceso, tarjetas de banda magnética, biometría, los sistemas biométricos de huellas dactilares, reconocimiento Geometría de la Mano, reconocimiento Facial

ABSTRACT

Today, access control more used to personnel entering the residential, it is done manually, where the guard makes a call to the apartment to which it is addressed, in order to authorize their entry, and if cleared it recorded in a log, just as the vehicle information.

Currently there are different systems for access Uto residential complexes such as magnetic cards, biometrics (fingerprint scan, iris scan, voice recognition, face, ear), some more expensive than others.

Therefore in this paper some tools used for access control to control the level of security in residential complexes, just as these systems keep updated database of personnel entering will be described.

Keywords: access control, magnetic stripe, biometrics, biometric systems fingerprint, hand geometry recognition, Facial recognition

INTRODUCCIÓN

Según las estadísticas del consejo colombiano de seguridad y la policía metropolitana de Bogotá, en el segundo eslabón de delitos de gran impacto en Colombia, se encuentra el robo a residencias con un reporte de 7.818 casos en todo el país para el primer cuatrimestre de 2015 frente a 6.503 que se registraron para el mismo periodo el año pasado, vemos un notable aumento en las estadísticas lo que nos lleva a buscar soluciones y estrategias que permitan disminuir estas cifras. En la mayoría de los casos la modalidad más utilizada por los delincuentes es la del ENGAÑO, la cual consistente en penetrar áreas restringidas en conjuntos residenciales bien sea haciéndose pasar por funcionarios autorizados o con técnicas como la llamada millonaria y suplantación. Sin embargo hoy en día en todos los sectores se busca cada vez más la comodidad "SEGURIDAD VS SERVICIO AL CLIENTE" y es que nuestro lugar de residencia no es la excepción. Todos quisiéramos llegar a nuestra casa sin pasar por ningún filtro de seguridad, que el domiciliario que nos lleva el almuerzo llegue lo más rápido posible y el plomero que llamamos no se pierda en el camino.

Hoy en día el control de acceso más utilizado al personal que ingresa a los conjuntos residenciales, se realiza manualmente, donde el vigilante hace una llamada al apartamento hacia el cual se dirige, con el fin que autorice su ingreso, y si es autorizado lo registran en una bitácora, de la misma forma la información de los vehículos.

Este registro no es muy confiable por que el personal encargado del control de acceso no cuenta con la información detallada del personal que va a ingresar al conjunto residencial, y más aún el riesgo se incrementa cuando hay cambios de turnos o rotan el personal, haciendo inseguro este

sistema, donde no se puede determinar en un momento explicito cuantas personas se encuentran dentro del conjunto residencial y detallar los registros históricos puntuales.

Por lo anterior la seguridad privada en servicio de vigilancia en un sector residencial, se puede fortalecer, y obtener ventajas cuando están a la vanguardia de los cambios constantes de los avances tecnológicos, ya que esta brinda herramientas que permiten minimizar los riesgos de inseguridad.

Es de suma importancia que para el ingreso a los conjuntos se implementen sistemas confiables, seguros, donde el ingreso del personal no se vuelva lento si no que por el contrario se agilice, se dejen registros y se minimicen los errores humanos.

Actualmente se cuenta con diferentes sistemas para el acceso a conjuntos residenciales como: tarjetas magnéticas, sistemas biométricos (escaneo de huella digital, escaneo del iris, reconocimiento de voz, cara, oreja), algunos más costosos que otros.

Por lo anterior en este trabajo se describirán algunas herramientas utilizadas para el control de acceso que permiten controlar el nivel de seguridad en los conjuntos residenciales, de igual manera estos sistemas mantienen actualizada la base de datos del personal que ingresa.

Un beneficio importante al implementar estos sistemas, es el incremento del grado de confianza, ya que no depende solo de la memoria o capacidad retentiva del personal de vigilancia, si no de bases de datos que los apoya para el almacenamiento de la información de los seres humanos que ingresan al conjunto residencial.

Estos sistemas facilitan el ingreso y la salida del personal, de una forma fácil y segura, de igual forma evita el ingreso a las personas no autorizadas y elimina los registros manuales por lo cual estos elementos son recomendables para el ingreso a los conjuntos residenciales que permiten

incrementar la seguridad del edifico, teniendo la certeza que únicamente ingresa el personal autorizado, donde se pueden ahorrar costos y gastos en personal especializado de vigilancia privada.

1. TARJETAS DE PROXIMIDAD

Estas tarjetas cuentan con una banda magnética, y una capacidad de memoria pequeña, que contiene un código para identificar rápidamente. La banda magnética fue inventada en 1960 por IBM, normalmente funcionan a una distancia entre 5 y 10 cm.

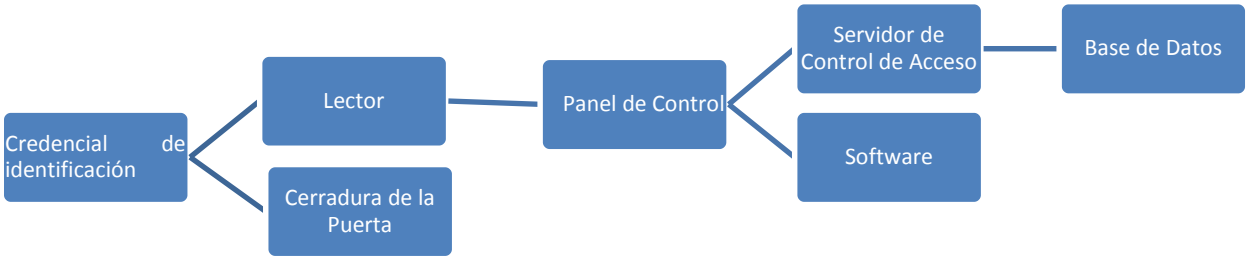
Gráfico 1 Tarjeta de Proximidad

Fuente: https://www.google.com.co/search?q=tarjetas+magneticas+de+proximidad&biw=1366&bih=667&

Estas tarjetas cada día tienen más aceptación y son las más utilizadas para el control de acceso, ya que permiten autenticar fácilmente la identidad de la persona, otorgándole al portador ciertos derechos y privilegios en el conjunto residencial, por lo que cada tarjeta almacena información, que se transmite al sistema, de tal forma que cuando la tarjeta se acerca al lector electrónico el acceso se brinda o se niega de acuerdo al perfil establecido, aunque esta tecnología disminuye costos, no garantiza que la persona que ingresa es la autorizada, de igual forma reduce la implicación del factor humano.

Este sistema de control de acceso está co-mpuesto por los siguientes elementos: Una tarjeta o ficha que se presenta al lector de la puerta de acceso, un lector de puerta de acceso que indica si la tarjeta es válida, cerradura de la puerta, un panel de control, servidor de control de acceso que autoriza la entrada y una puerta de acceso o portón, que abre cuando se autoriza la entrada, un software y una base de datos.

Gráfico 2 .Componentes Sistemas de Control de Acceso Tarjeta Inteligente



Fuente: el autor

Esto inicia cuando el personal autorizado pasa la tarjeta al lector, que normalmente está cerca a la puerta o portón de entrada, el lector extrae los datos de la tarjeta inteligente y los procesa, enviándolos al panel de control, donde este valida el lector, luego acepta los datos transmitidos por el lector y transmite los datos al servidor, el servidor compara los datos recibidos de la tarjeta con la información que se encuentra almacenada en la base de datos y el programa determina los privilegios de acceso y su perfil, la hora, la fecha, y la puerta a la que va a ingresar y cualquier otra información que se necesite para fortalecer la seguridad.

Cuando se autoriza el ingreso, el servidor envía una señal al panel de control que permite abrir la puerta donde el panel de control normalmente envía unas señales la primera es a la cerradura de la puerta para que se pueda abrir, la segunda es en el lector de la puerta emitiendo un sonido o cambiando el color en el lector de la puerta o cualquier otra señal indicando que ya se puede ingresar, o por el contario niega el acceso. El panel de control recopila información sobre los datos de las tarjetas proporcionando un flujo de información que se usa para tomar decisiones de control de acceso y contar con información oportuna.

Las tarjetas de identificación magnéticas son una solución económica y que atienden a los requerimientos de los conjuntos residenciales donde se puede dar acceso limitado a áreas restringidas o especiales al personal que ingresa.

2. SISTEMAS BIOMÉTRICOS

Antecedentes de la Biometría

Reportes de João de Barros en el siglo XIV en el país de China, los mercaderes timbraban las huellas de la palma de la mano y los pies de los niños en un papel con tinta con el fin de lograr diferenciar un niño de otro. En 1686 el Italiano Marcello Malpighi, fue el primero que identificó que los patrones de la piel en los dedos eran totalmente diferentes y en 1823 Jan Evangelista Purkine, médico y científico de la ciudad de Checoslovaquia identificó la naturaleza única de las huellas digitales de los individuos, el identificó las espirales, elipses y triángulos en las huellas digitales.

En 1858 William Herschel, trabajador del servicio civil de la India, estampó la huella de la mano al reverso de un contrato para cada uno de los trabajadores con el fin de distinguir los unos de los otros y que pretendieran suplantar a los trabajadores el día de pago.

En 1882, con el policía francés Alphonse Bertolli presentó por primera vez un sistema de identificación de personas basado en las características físicas donde se exponen rasgos biométricos, lo llamó antropometría, siendo el primer sistema científico que uso la Policía para identificar criminales iniciándose con la clasificación de la nariz, la cara o el cuerpo del ser humano.

En 1930, en la Universidad de Harvard desarrolla algoritmos para el reconocimiento Biométrico a través del patrón de iris, en 1941, Murria Hill en los laboratorios Bell, inició el estudio de identificación de voz, en 1960 se da a conocer el reconocimiento y autenticación de una persona a través de la mano.

En 1989: El National Institute Standards and Technology de EEUU comenzó a desarrollar métodos para experimentar sistemas biométricos, en 1994 se patentó el algoritmo sobre reconocimiento de patrón de iris.

Los sistemas que se basan en la verificación de voz, escritura, huellas, patrones oculares (retina-iris), geometría de la mano, entre otros son llamados biométricos. Por lo anterior la Ley 16 de 2014 define como la aplicación de técnicas matemáticas y de estadísticas sobre los rasgos físicos o de conducta de un individuo para su autentificación, es decir, "verificar" su identidad. La palabra biometría se deriva de la palabra griego bios de vida y metron de medida. La biometría permite la certificación, autentificación e identificación de personas en sistemas de seguridad.

Francesc Serratosa (2013) en su libro la biometría para identificación de las personas define el reconocimiento biométrico como:

El uso de diferentes características anatómicas (como huellas dactilares, cara o iris) y de comportamiento (como habla, firma o teclear). Estas características se denominan

identificadores biométricos o rasgos biométricos y sirven para reconocer automáticamente a los individuos. (p.14).

Hoy en día la sociedad ha avanzado donde actualmente está conectada electrónicamente y es cada vez más móvil, donde la identificación de personas por medio de códigos y tarjetas no son confiables para establecer la identidad de los seres humanos, los códigos se pueden adivinar y las tarjetas se pueden perder o se las pueden robar, de igual forma los códigos y tarjetas se pueden compartir entre los amigos y compañeros de trabajo, por lo anterior las tarjetas y los códigos no garantizan la identidad de las personas.

La utilización de la biometría se ha convertido en un instrumento esencial para la identificación eficaz de los seres humanos, esto se debe a que los rasgos biométricos no se pueden compartir o perder, ya que se reconoce la persona por medio de su cuerpo para que se pueda enlazar con una identidad determinada en una tecnología, que permite fortalecer la seguridad y reducir el fraude.

Para que exista un sistema biométrico es necesario que cumpla con las siguientes características:

- Universalidad: Es donde todas las personas deben contener las mismas características.
- Unicidad: Dos personas no pueden ser la misma en los requisitos de las características.
- Permanencia: Las características no pueden variar con el tiempo.
- Cuantificable: Estas características pueden ser medidas cualitativamente.
- Realización: Se refiere a si es posible le identificación exacta, los recursos necesarios y los diferentes factores del entorno.
- Aceptabilidad: Va dirigido a la población que estaría dispuesta a aceptar este sistema de identificación.
- Engañable: describe cual fácil el sistema se puede engañar con técnicas fraudulentas.

Las ventajas generales de estos sistemas biométricos se basan en que son fáciles de usar de tal forma que el usuario no tiene nada que recordar, nada que cambiar y nada que perder, eleva el nivel de seguridad ya que cuenta con una característica humana que no puede ser fácilmente adivinada o descifrada, algunas características son inalterables y también imposibles de transferir u olvidar lo que hace que el sistema sea confiable, amigable y seguro ya que tienen una precisión y velocidad aceptable en comparación a las tarjetas magnéticas.

Cada sistema biométrico cuenta con sus propias características, variedades y certezas. Los niveles de precisión son más confiables que las tarjetas o contraseñas. La verificación certera de la identidad de las personas que ingresa a los conjuntos residenciales puede minimizar el riesgo de la delincuencia y el fraude.

En los sistemas biométricos se pueden identificar dos tipos de sistemas: sistemas de verificación y sistemas de identificación. Francesc Serratosa (2013) define sistemas de verificación o también llamados de autentificación como el sistema donde se "autentifican la identificación de la persona mediante la comparación del rasgo biométrico acabado de capturar con el rasgo biométrico que el sistema ha capturado antes en el proceso de inscripción al sistema". (p.17).

Los sistemas de identificación Francesc Serratosa (2013) dice que son: "los que reconocen a la persona a través de la búsqueda del rasgo biométrico que más se asemeja al usado para identificarlo en toda una base de datos". (p.17).

Por lo anterior en el sistema de verificación la persona aporta una información de su identificación y en el sistema de identificación se lleva a cabo una comparación del rasgo biométrico en una base de datos. Estos dos sistemas necesitan un proceso previo el cual es llamado sistema de matriculación, Francesc Serratosa (2013) indica que "Este proceso se encarga de

recoger el rasgo biométrico junto con la identificación de la persona., es muy importante puesto que se encarga de relacionar la identificación de la persona con el rasgo biométrico. (p.18).

Para llevar a cabo el sistema de identificación, verificación y matriculación Francesc Serratosa (2013) explica que se deben llevar acabo los siguientes procesos:

- Captura: es la representación digital del rasgo biométrico que debe ser capturada.
- Extracción de las características: tiene como finalidad facilitar la comparación, aumentar la información, y reducir el ruido de la representación original digital.
- Creación de la plantilla: se recibe la entrada de los registros de identificación y se crea una información compacta, donde se extraerá la información de todas las muestras que se consideran rasgos característicos.
- Comparación: se recibe como entrada un registro de identificación y una plantilla, con una distancia que debe calcular entre los dos.
- Selección o filtrado: en la base de datos existe información donde se filtra de acuerdo a los rasgos de identificación ingresados.
- Almacenamiento de los datos: es donde se almacena la información y que está constituida con los siguientes datos: identificados único, plantilla biométrica, y otros datos como dirección y teléfono

El dominio de un sistema biométrico puede operar por un sistema lineal o sistemas fuera de línea. Los sistemas de línea es cuando la comparación se lleva a cabo rápidamente y hay una respuesta inmediata, son automáticos, se capturan por medio de un sensor automático y no hay un control humano. Un sistema fuera de línea, la respuesta no es inmediata y se permite el retraso de la respuesta, son sistemas semiautomáticos, la captura del rasgo de identificación puede haber sido

en un sistema no electrónico. El sistema óptimo para los conjuntos residenciales es el sistema en línea.

En este trabajo se hará una descripción de lectores de huellas digitales y el reconocimiento facial.

Existe una gran variedad de sensores que son utilizados para los sistemas biométricos, se define como sensor: un dispositivo que detecta manifestaciones de cualidades físicas tales como la energía, cantidad, velocidad entre otros. Para cada característica deseada existe un sistema de captación, por ejemplo para el rostro es necesario una cámara, para el reconocimiento de voz se utiliza un micrófono, entre los sensores más destacados podemos encontrar:

Sensores ópticos: Son los que detectan los elementos por medio de un lente óptico un claro ejemplo es el mouse del computador ya que por medio de este lente se mueve el cursor de acuerdo a los movimientos que se le indican. Estos sensores se encuentran conformados por: fuente, receptor, lentes y circuito de salida.

Sensores termoeléctricos: Es un procedimiento poco utilizado, actualmente es manejado en el mercado Atmel Fingerchip, que aprovecha para el reconocimiento de la huella dactilar. Este sistema reproduce el dedo completo cuando se pasa por sensor el cual mide la temperatura entre las crestas capilares y el aire que se retienen entre los surcos.

Sensores capacitivos: Es uno de los utilizados y reconocidos para la huella dactilar, este escáner genera una imagen de la cresta y los valles del dedo.

Sensores de campo eléctrico: Este sensor funciona a través de una antena que mide el campo eléctrico entre 2 capas conductoras. Esta herramienta tecnológica fue creada para que su

funcionamiento se adapte a cualquier condición en la que se encuentre el dedo por ejemplo que su piel este húmeda o seca.

Sensores sin contacto: Este sensor funciona de forma similar a los sensores ópticos, casi siempre con un cristal de precisión óptica a una distancia entre dos o tres pulgadas de la huella dactilar mientras se escanea el dedo.

2.1 Lectores de Huellas Digitales

El ministerio del Interior del Reino Unido en 1893 aceptó oficialmente que dos personas no podían tener exactamente las mismas huellas dactilares, información que los departamentos de policía utilizaron para identificar infractores o criminales donde iniciaron las comisarías de policía a crear archivos de criminales a través de sus huellas dactilares.

Los lectores de huellas digitales se pueden utilizar para abrir puertas de garajes, cerraduras, donde no es necesario contar con una llave, si no con un lector biométrico, por lo que establece las siguientes ventajas: eliminar suplantaciones de identidad y controlar el ingreso de personas no autorizadas a la entidad, no existen riesgos de falsificación, el medio de identificación es único y personal, además hoy en día es una tecnología muy fácil de instalar y económica.

La huella dactilar se define como la impresión visible o moldeada que produce el contacto de las crestas papilares de un dedo de la mano sobre una superficie, la forma que cubre la piel de la yema de los dedos está constituida por formar salientes y depresiones, las salientes son llamadas crestas papilares y las depresiones surcos inter papilares. En las crestas se encuentran glándulas sudoríparas, de tal forma que este sudor produce un aceite que los retienen los surcos de las huellas y cuando el dedo hace contacto con la superficie produce un negativo de la huella.

Esto funciona capturando la huella digital y los datos básicos del personal al ingresar al conjunto residencial, proceso que dura máximo 30 segundos, la información se almacena y procesa por un algoritmo numérico en la base de datos, quien dará los permisos respectivos para ingresar a ciertas áreas.

Este tipo de tecnología ha venido incursionando en el acceso a conjuntos residenciales ya que incrementa los niveles de seguridad donde a las personas no autorizadas el sistema no les permite el ingreso.

Para la implementación se requiere una buena programación del hardware y software, ya que son los factores determinantes para la funcionalidad de este sistema. Los elementos necesarios son los siguientes:

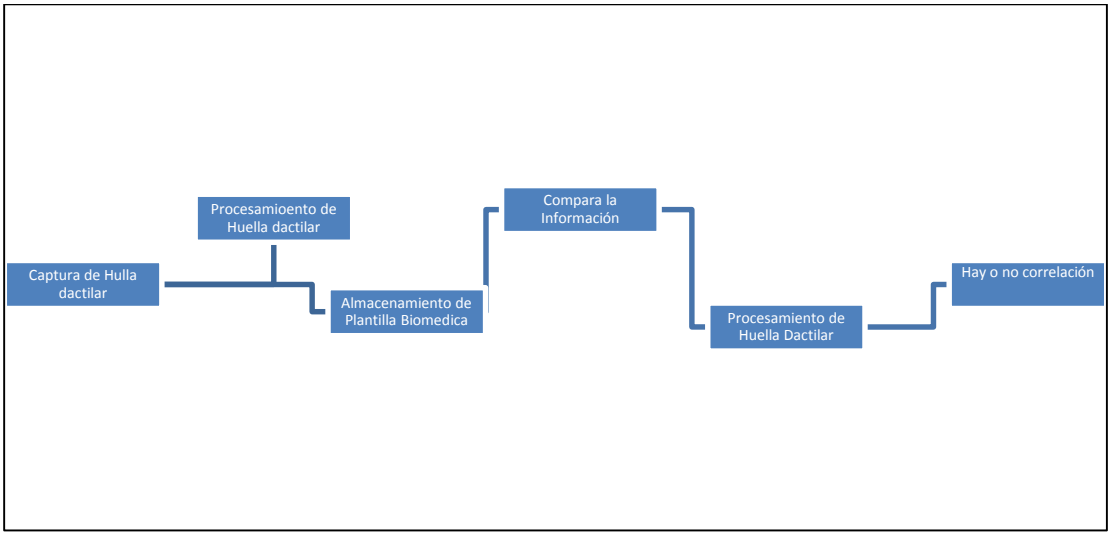
- Requerimiento de un Hardware: se refiere a un lector de huella digital que se asocia a una computadora y funciona como terminal para registrar el acceso del personal. Este lector de huella tiene como función obtener la imagen de la huella digital y comparar los valles y crestas de la imagen cuando tiene patrones de huellas almacenados.

Gráfico 3 . Captura de Huella

Fuente: ttp://www.archiexpo.es/prod/bioaccez-controls-sl/lector-huella-digital-control-acceso-58916-729796.html

- Requerimiento de un Software: analiza las características y las convierte en un identificador numérico, luego compara los patrones que se han extraído en el proceso almacenándolos en el sistema¸ la salida puede dar como resultado la semejanza de la característica almacenada con la característica de la persona en comparación y la toma de decisión siendo el resultado de la comparación del resultado positivo que va a permitir el acceso o de lo contrario es denegado, afirma o niega el usuario es quien dice ser.

Gráfico 4 . Proceso del funcionamiento de Sistema Biométrico de la Huella dactilar

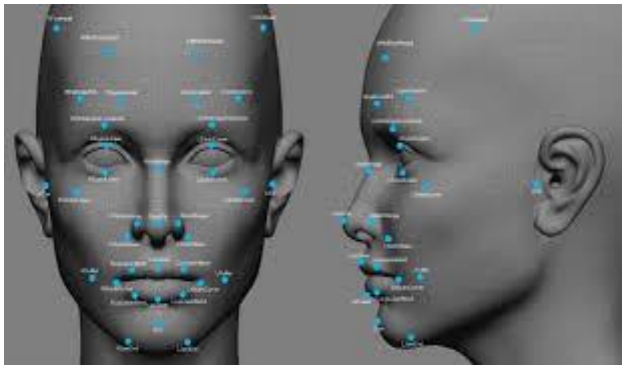


Fuente: el autor

Dentro de las ventajas de este sistema es que es muy seguro, capturando un punto de identidad que es difícil de falsificar, de la misma forma es un código que siempre lo lleva consigo, que no se puede olvidar y muy difícil de perder, una de las grandes desventajas es que estos sistemas son costosos de implementar, lo que puede excluir muchos conjuntos residenciales.

2.2 Reconocimiento Facial

Gráfico 5. Reconocimiento Facial



Fuente:https://www.google.com.co/search?q=como+funciona+biometria+facial&biw=1571&bih

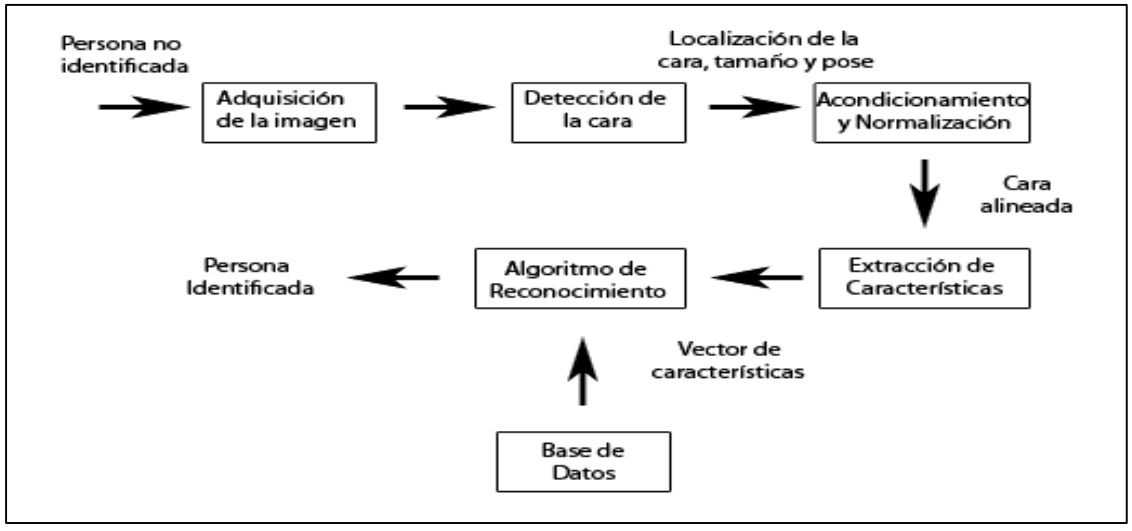
Este sistema extrae los rasgos faciales de los usuarios para su identificación. Es una técnica que consiste en que dada una imagen desconocida de una cara el sistema debe encontrar una imagen de la misma cara en un conjunto de imágenes conocidas. Este reconocimiento facial es un concepto relativamente nuevo. Esta tecnología predomina en dos enfoques: el geométrico y el fotométrico. El geométrico se basa en rasgos y el fotométrico se basa en lo visual.

El proceso consta de cuatro módulos que son: Detección de la cara, Alineación de la cara, Extracción de características, Reconocimiento.

- Detección de la cara: es cuando detecta la cara en la imagen.
- Alineación de la cara: localiza los elementos de la cara, y a través de transformaciones geométricas la normaliza en cuanto a propiedades geométricas, en su tamaño, pose y fotométrica.
- Extracción de características: en este modelo se proporciona información con el fin de distinguir entre las diferentes caras de la persona de acuerdo a las variaciones geométricas o fotométricas.

- Reconocimiento: el vector de la cara que extrajo se compara con los vectores extraídos de las diferentes caras de la base de datos. Si encuentra un porcentaje elevado de igualdad abre el control de acceso si no, indica que es una cara desconocida.

Gráfico 6. Sistema de Reconocimiento Facial



Fuente: https://misproblemasdemate.wordpress.com/2014/01/04/valores-y-vectores-propios/

Una de las principales debilidades de este sistema se debe al ángulo en que se encuentre al rostro el cual se desea reconocer, otro inconveniente es en lugares donde exista poca luz, más aun cuando la persona lleva pelo largo, o gafas.

2.3 Reconocimiento Geometría de la Mano

La Real Academia Española define a la mano "como una parte del cuerpo humano unida a la extremidad del antebrazo y que comprende desde la muñeca hasta la punta de los dedos". La mano está compuesta en un esqueleto óseo, que se encuentra dotado por veintisiete (27) huesos articulados entre sí.

Gráfico 7. Sistema de Reconocimiento Geométrico de la Mano

Fuente: http://www.biosys.es/productos/handkey-i-d3d/

La mano consta de tres grupos de huesos: los del carpo, metacarpo y dedos. El carpo es la parte más cercana a la mano, vecina de la muñeca, y consta de ocho huesos dispuestos en dos filas, cuatro en cada una. El segundo grupo está formado por los cinco metacarpianos y forman la parte más distal del esqueleto de la palma. El tercer grupo, los dedos, está constituido por los huesos de los dedos, las falanges, pequeñas y cortas, de las que hay tres en cada dedo, exceptuando el pulgar que tiene dos. Los músculos de la mano se dividen fundamentalmente en dos grupos: flexores, los de la cara palmar, y extensores, los de la dorsal.

El primer sistema comercial para reconocimiento de geometría de mano se adecuo a principios de los años 70. La Universidad de Georgia fue una de las primeras instituciones en utilizarlo en 1974. El ejército de Estados Unidos lo probó para su uso en bancos en 1984, pero el concepto no fue patentado hasta 1985. David Sidlauskas desarrolló y patentó el concepto de geometría de la mano en 1985 creando al mismo tiempo la empresa Recognition Systems Inc., cuyo primer sistema

comercial estuvo disponible al año siguiente. En los Juegos Olímpico de 1996 se hizo uso de este tipo de sistemas para controlar y proteger el acceso físico a la Villa Olímpica[1].

Los sistemas biométricos utilizan la imagen de la mano ya sea la derecha o la izquierda donde se definen unas características que son basados de acuerdo a la geometría de la mano, en los surcos de la palma de la mano, en la geometría de los dedos, en el contorno de la mano, en los nudillos de los dedos, en la geometría tridimensional, entre otros.

Este proceso se realiza por medio de un dispositivo que contenga un conjunto de pequeños pivotes que controlan la posición de la mano, de tal forma que cuando se coloca la mano, se toman las imágenes de la parte anterior y posterior, con el fin de realizar la extracción de las características de la mano.

Gráfico 8. Reconocimiento Geométrico de la mano

Fuente: https://www.google.com.co/search?q=sistema+biometrico+de+geometria+de+la+mano&rlz=1C1

El proceso de extracción de características comienza con la obtención del sistema de referencia de la mano. Para ello es necesaria una previa la imagen de la mano respecto al eje de la imagen. De forma que la mano es posicionada dentro de la imagen con una orientación concreta ya que la mano ha sido capturada en la disposición libre con la que el usuario la colocó en la plataforma.

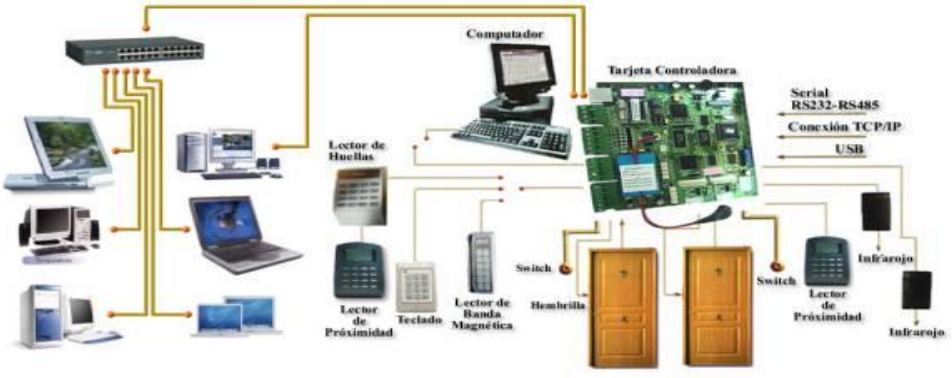
[1] http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas/recomano.html

2.4 Filosofía de Control de Accesos con enfoque del sector residencial

La filosofía de control de accesos en el sector residencial debe estar combinada con la tecnología, ya que esto permite aumentar la seguridad de los conjuntos residenciales, incrementar las barreras control y de igual forma contar con información oportuna.

Estos sistemas de control de accesos se desarrollan para tener el control de todo el personal que transita en los conjuntos residenciales, asegurando el paso de personas que cuentan con un libre tránsito y restringiendo el paso de personas no autorizadas en áreas específicas. Las soluciones para control de accesos son variadas dependiendo de las aplicaciones y las necesidades de cada conjunto, se pueden tener desde soluciones con un solo dispositivo que controla una puerta, hasta soluciones con múltiples dispositivos integrados a diferentes sistemas electromecánicos gestionados por medio de software centralizado.

Gráfico 9. Control de acceso sector residencial



Fuente:https://www.google.com.co/search?q=diagrama+Control+de+Accesos++sector+residencial&rlz=1C1CHM

Este sistema permite incrementar la seguridad del edificio, teniendo la certeza que únicamente ingresan personas autorizadas, ahorrar en los costos y gastos fijos en personal especializado de vigilancia privada, agilidad en los tiempos de entrada y salida ya que el personal autorizado

esta previamente registrado en las bases de datos y no se tiene que hacer un registro completo diario, mayor control y gestión de todo el personal, trabajadores y visitantes e integración con todos los sistemas de seguridad para lograr una gestión más eficiente de todo el edificio.

2.5 Garita de Seguridad

Como último complemento de este trabajo, se dan a conocer a continuación algunos aspectos que deben tenerse en cuenta al momento de instalar garitas en los conjuntos residenciales con el propósito de generar seguridad en el área incluye sistema de vigilancia especializado y capacitado de acuerdo con los estándares del conjunto, y aislamiento de la zona de cajeros de modo tal que no se permita el ingreso de los delincuentes en esta zona.

Entre las características se encuentran las siguientes:

La garita de seguridad se debe construir y situar estratégicamente y ser dotadas de medios básicos para la prestación del servicio de vigilancia, se deben construirse en materiales resistentes a grandes impactos, tanto de arma como de elementos contundentes, el diseño debe tener como mínimo adecuada visibilidad al exterior, los ventanales deben instalarse con vidrio resistente a armas de fuego, debe contar con un mecanismo de comunicación principal.

CONCLUSIONES

Como se describe anteriormente estas herramientas son utilizadas actualmente para el control de acceso, lo que permite incrementar, fortalecer y controlar el nivel de seguridad en los conjuntos residenciales, obteniendo que sean registros confiables, disminuyendo los riesgos de inseguridad, por medio de las ventajas de los avances tecnológicos se logra minimizar los errores humanos.

La seguridad física demanda hoy en día un mejor control de personal, lo que permite apoyar los niveles de seguridad en los conjuntos residenciales, por lo anterior estas herramientas bien parametrizadas incrementan la seguridad de los conjuntos ya que no dependen únicamente de la memoria y retentiva de los vigilantes y del riesgo que existe de la rotación de estos. Este factor humano se puede utilizar para fortalecer otras áreas como monitorear el circuito cerrado de televisión

La instalación de tecnologías para el control de acceso en los conjuntos residenciales facilita rápidamente el acceso, cada sistema se debe ajustar a las necesidades del conjunto, ya sea por medio de tarjetas magnéticas o sistemas biométricos.

La tecnología debe permitir mejorar la calidad en la prestación de los servicios de Vigilancia y seguridad privada, asegurando un adecuado nivel técnico y profesional

Estos sistemas minimizan el riesgo de intrusión, herramientas que sirven de apoyo al personal de vigilancia y ayudan a controlar el acceso de una manera eficiente de los conjuntos residenciales.

Lo importante es determinar su costo, comodidad en el momento, seguridad de instalaciones, ahorro de tiempo, restringir el acceso al personal no autorizado, hacer los registros necesarios que se deben realizar durante el servicio y que se logre indicar las fechas y horas.

El control de acceso a la copropiedad va desde los más económicos que son las tarjetas de proximidad, hasta los más robustos que son los biométricos (Huella dactilar, reconocimiento facial), en esta tecnología debe existir un hardware y un software

La biometría por medio de huellas dactilares es la más conocida que se ha utilizado para el reconocimiento humano, donde la identificación se basa en las bifurcaciones de las crestas.

Uno de los beneficios de los sistemas biométricos es que las personas llevan consigo el rasgo que los identifica en el sistema. De igual manera para el reconocimiento es necesario un registro, una identificación y una verificación.

No existe una herramienta 100% segura, sin embargo se recomienda que los conjuntos residenciales utilicen una combinación de los controles para el acceso que logre minimizar la falsificación o suplantación, esta composición podría ser con la tarjeta de control más un lector biométrico.

De igual forma realizar una combinación de más de dos herramientas lo hace muy complejo y muy lento, por lo que no es recomendable esta composición.

El riesgo de esta tecnología es la idoneidad de la implantación de estos sistemas, por lo que es necesario un análisis previo para llevar a cabo la implementación de los sistemas adecuados para los conjuntos residenciales, de igual forma se encuentra la suplantación de identidad con las tarjetas de acceso, la alteración de rasgos con los sistemas biométricos, el desconocimiento de la calidad y las utilidades del sistema y la percepción negativa por parte de los usuarios.

BIBLIOGRAFÍA

Galiacho, J. (1998). *Herramientas para vigilantes* . Obtenido de Casa del libro: http://www.casadellibro.com/libro-herramientas-para-vigilantes-area-juridico-y-social/9788428324793/615626

Álvarez , A. (2005). *Hablemos de seguridad.* Cartagena de Indias: Ediciones Pluma de Mompox,.

Bernal, R. (1996). *Auditoria En Los Sistemas De Información.* España: Reproval .

Casal, J. (2001). *Análisis de Riesgo En instalaciones Industriales.* Bogotá: Alfa.

Chopra, S. (2008). *Administración de la Cadena de Suministrios.* Recuperado el 2014, de http://catalogo.unimilitar.edu.co/cgi-bin/koha/opac-detail.pl?biblionumber=11358&query_desc=seguridad%20fisica%20%23title_az

Niles, S. (2004). *Seguridad Física en Instalaciones de Importancia Critica.* White paper 82, Revisión 2.

Política seguridad física SISTESEG, Bogotá Colombia. (s.f.). Recuperado el 2014, de http://www.sisteseg.com/files/Microsoft_Word_-_Politica_Seguridad_Fisica.pdf

Ramirez, c. (2005). *Seguridad Industrial.* México: Limusa.

Ley No 16 . *Por la cual se implementan el Sistema de Ideentificación Biométrico en los aeropuesrtos, terminales de transporte terrestre y martitimos a nivel nacional y se dictan otras dispociones,* Diario oficial Graceta 376 de 2014